UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/569,530	02/24/2006	Sturla Lutnaes	956315	6019

54414 7590 10/27/2008

MYERS BIGEL SIBLEY & SAJOVEC, P.A.
P.O. BOX 37428
RALEIGH, NC 27627

EXAMINER	
SHOLEMAN, ABU S	

ART UNIT	PAPER NUMBER
4148	

MAIL DATE	DELIVERY MODE
10/27/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/569,530	LUTNAES, STURLA	
	Examiner	Art Unit	
	ABU SHOLEMAN	4148	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *02/24/2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-27* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-27* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on *02/24/2006* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *02/24/2006*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This instant application having Application No. 10569530 filed on 02/24/2006 is presented for examination by the examiner.

Oath/Declaration

2. The applicants' oath/declaration has been reviewed by the examiner and is found to conform to the requirements prescribed in **37 C.F.R.1.63.**

Priority

3. As required by **M.P.E.P.201.14(c),** acknowledgement is made of applicant's claim for priority based on applications filed on September 02, 2003 (EPO 03019882.4).

Information Disclosure Statement

4. The information disclosure statement (IDS) submitted on 02/24/2006 has been acknowledged. The submission is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Drawings

5. The drawings were received on 02/24/2006. These drawings are acceptable for examination purposes.

Claim Rejections - 35 USC § 112

6. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

7. Claims 4,9,12,13 and 22 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 4 recites the limitation “the pre-defined area” in line 4. there is insufficient antecedent basis for this limitation resulting in indefiniteness in the claim. It is not clearly understood how "the pre-defined area" relates to “pre-defined” of line 3 of claim 4.

Claim 9 recites the limitation “the data processing environment ” in line 11. there is insufficient antecedent basis for this limitation resulting in indefiniteness in the claim. It is not clearly understood how "the data processing environment " relates to “an electronic data processing “ of line 9 of claim 2.

Claim 12 recites the limitation “the pre-defined area” in line 5. there is insufficient antecedent basis for this limitation resulting in indefiniteness in the claim. It is not clearly understood how "the pre-defined area" relates to “pre-defined” of line 3 of claim 12.

Claim 13 recites the limitation “the pre-defined area” in line 4. there is insufficient antecedent basis for this limitation resulting in indefiniteness in the claim. It is not clearly understood how "the pre-defined area" relates to “pre-defined” of line 2 of claim 13.

Claim 22 recites the limitation “the pre-defined area” in line 5. there is insufficient antecedent basis for this limitation resulting in indefiniteness in the claim. It is not clearly understood how "the pre-defined area" relates to “pre-defined” of line 3 of claim 22.

Claim Rejections - 35 USC § 102

7. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

8. Claims 1-6, 8-13,15,16,18-22 and 24-27 are rejected under 35 U.S.C 102(b) are being anticipated by Anderson (Patent number: 6115819)(hereinafter Anderson).

As per claim 1, Anderson discloses "A method of transferring data from a non-volatile memory to a working memory of an electronic data processing device" as (Fig 1, Transferring data from ROM 12 to Main RAM 30). "copying security data from the non-volatile memory to the working memory, wherein the security data is to be write-protected" as (column 6, line 15-19, exchanging data between various elements of the system);"activating a blocking function for the security data in the working memory, wherein activating is triggered by the copying being made to the working memory" as (column 4, line 46-50, the Access monitor is being initiation at the time of copying data from ROM to Main RAM); "monitoring all communication with the working memory" as (column 4, line 59-61, By monitoring the signals on the system bus the access monitor can

determine the details of every data access that takes place); and "blocking all write attempts to the copied security data stored in the working memory according to the blocking function, wherein at least activating a blocking function ,monitoring communication and blocking write attempts performed independently of a central processing unit of the electronic data processing device, such that the central processing unit cannot manipulate the security data " as (column 6. line 46-48, The AM will allow or disallow the access to memory by controlling gate 44 to pass or not pass the read or write command, column 6, line 15-19,Restrictions on the exchange or transfer of data between various elements of the system is controlled by the Access monitor).

As per claim 2, Anderson discloses " wherein an area of the security data in the non-volatile memory is pre-defined and pre-stored in a device for blocking write attempts and used at least in relation to activating a blocking function" as (column 6, line 46-48,Fig 1, ROM is stored with pre-defined data , The AM blocks the write attempt to the RAM).

As per claim 3, Anderson discloses " copying data comprises copying only the security data from the non-volatile memory to the working memory independently of the central processing unit of the data processing device and coping any further data under the control of the central processing unit of the device" as (column 6, line26-31,Fig 1, in order to copy data from ROM to RAM

under the unit CPU , because CPU sends a signal to the AM that look up the Tag which is associated with memory location in RAM).

As per claim 4, Anderson discloses " wherein an area of the security data in the non-volatile memory and an area for storage of the security data in the working memory are pre-defined and wherein activating a blocking function is triggered by the copying being made to the pre-defined area in the working memory and the blocking function is activated for that area of the working memory" as (column 6, line 25-30, When CPU copy pre-defined data area from ROM to RAM , then it sends a signal to triggered the AM in order to activate during the copying data into Memory).

As per claim 5, Anderson discloses " copying comprises copying all data from the non-volatile memory to the working memory under the control of the central processing unit of the device" as (column 8, line 21-25, When the AM is allowing to copy data from ROM to RAM that will be allowed by the CPU).

AS per claim 6, Anderson discloses " wherein an area of the security data in the non –volatile memory is pre-defined and wherein activating a blocking function is triggered by a first detection of copying of security data from the pre-defined area in the non-volatile memory to an area of the working memory and blocking function is activated for that area of the working memory" as (column 6,

line 30-33, During copying data from ROM to RAM , CPU sends a signal 58 to trigger the AM for accessing the tag memory 56 to active the area of the RAM).

As per claim 8, Anderson discloses "Disconnecting a debugging unit at least when copying the security data to the working memory and reconnect the debugging unit when the blocking function has been activated" as (column 4, line 59-67, Fig 1, The gate 44 is disable when the CPU is copying the data from ROM to Main RAM, The gate 44 is enabled when the AM is triggered).

As per claim 9, Anderson discloses " A device for blocking write attempts to security data transferred from a non-volatile memory to a working memory in an electronics data processing environment that includes a central processing unit and comprising a monitoring unit" as (Fig 1),"activating a blocking function for the security data in the working memory, which activation is triggered by the copying being made to the working memory" as (column 4, line 46-50, the Access monitor is being initiation at the time of copying data from ROM to Main RAM); "monitoring all communication with the working memory" as (column 4, line 59-61, By monitoring the signals on the system bus the access monitor can determine the details of every data access that takes place);and "blocking all write attempts to the copied security data stored in the working memory according to the blocking function, all performed independently of the central processing unit of the data processing environment such that the central processing unit cannot manipulate the security data " as (column 6. line 46-48,

The AM will allow or disallow the access to memory by controlling gate 44 to pass or not pass the read or write command, column 6, line 15-19, Restrictions on the exchange or transfer of data between various elements of the system is controlled by the Access monitor and CUP can not modify the data in the RAM because it would not get access permission from the AM).

As per claim 10, Anderson discloses "wherein an area of the security data in the non-volatile memory is pre-defined and pre-stored in a device and used at least in relation to activating a blocking function" as (column 6, line 46-48,Fig 1, ROM is stored with pre-defined data , The AM blocks the write attempt to the RAM).

As per claim 11, Anderson discloses " a copy control unit configured to copy the security data from the non-volatile memory to the working memory also independently of the central processing unit of the data processing environment" as (column 6, line26-31,Fig 1, in order to copy data from ROM to RAM under the unit CPU , because CPU sends a signal to the AM that look up the Tag which is associated with memory location in RAM).

As per claim 12, Anderson discloses " wherein and area of the security data in the non-volatile memory and an area for storage of the security data in the working memory are pre-defined and pre-stored in the device and the monitoring unit when activating a blocking function is triggered by the copying being made to the pre-defined area in the working memory and the blocking

function is activated for that area of the working memory" as (column 6, line 25-30, When CPU copy pre-defined data area from ROM to RAM , then it sends a signal to triggered the AM in order to activate during the copying data into Memory).

As per claim 13, Anderson discloses " wherein an area of the security data in the non-volatile memory is predefined and pre-stored in the device and the monitoring unit when activating of blocking function is triggered by a first detection of copying of security data from the pre-defined area in the non-volatile memory to an area of the working memory and the blocking function is activated for that area of the working memory" as (column 6, line 30-33, During copying data from ROM to RAM , CPU sends a signal 58 to trigger the AM for accessing the tag memory 56 to active the area of the RAM).

As per claim 15, Anderson discloses " wherein the monitoring unit is configured to disconnect a debugging unit of the electronic data processing environment at least when the security data is copied to the working memory and to reconnect the debugging unit when the blocking has been activated" as (column 4, line 59-67, Fig 1, The gate 44 is disable when the CPU is copying the data from ROM to Main RAM, The gate 44 is enabled when the AM is triggered).

As per claim 16, Anderson discloses "wherein it is implemented in hardware" as (column 6, line 3-4,Fig 1, The architecture of the peripheral device).

As per claim 18, Anderson discloses “wherein an area of the security data in the non-volatile memory is pre-defined and pre-stored in the device for blocking write attempts and used at least in relation to activating a blocking function" as (column 6, line 46-48,Fig 1, ROM is stored with pre-defined data , The AM blocks the write attempt to the RAM

As per claim 19, Anderson discloses “ wherein the device for blocking write attempts further comprises a copy control unit configured to copy the security data from the non-volatile memory to the working memory also independently of the central processing unit of the data processing environment" as (column 6, line26-31,Fig 1, in order to copy data from ROM to RAM under the unit CPU , because CPU sends a signal to the AM that look up the Tag which is associated with memory location in RAM).

As per claim 20, Anderson discloses “ wherein area of the security data in the non-volatile memory and the area for storage of the security data in the working memory are pre-defined and pre-stored in the device and the monitoring unit when activating a blocking function is triggered by the copying being made to the pre-defined area in the working memory and the blocking function is activated for that area of the working memory" as (column 6, line 25-30, When CPU copy

pre-defined data area from ROM to RAM , then it sends a signal to triggered the AM in order to activate during the copying data into Memory).

As per claim 21, Anderson discloses “wherein the central processing unit is configured to control the copy of all data from the non-volatile memory to the working memory” as (column 6, line 20-23, The CPU is configured to access memory by The AM).

As per claim 22, Anderson discloses “ wherein an area of the security data in the non-volatile memory is predefined and pre-stored in the device and the monitoring unit when activating of blocking function is triggered by a first detection of copying of security data from the pre-defined area in the non-volatile memory to an area of the working memory and the blocking function is activated for that area of the working memory" as (column 6, line 30-33, During copying data from ROM to RAM , CPU sends a signal 58 to trigger the AM for accessing the tag memory 56 to active the area of the RAM).

As per claim 24, Anderson discloses "further comprising a debugging unit and wherein the monitoring unit is configured to disconnect the debugging unit at least when the security data is copied to the working memory and to reconnect the debugging unit when the blocking has been activated" as (column 4, line 59-67, Fig 1, The gate 44 is disable when the CPU is copying the data from ROM to Main RAM, The gate 44 is enabled when the AM is triggered).

As per claim 25, Anderson discloses "wherein the device for blocking write attempts is implemented in hardware" as (column 6, line 3-4,Fig 1, The architecture of the peripheral device).

As per claim 26, Anderson discloses “where in the device is a portable communication device” as (see Abstract , a respective gateway device).

As per claim 27, Anderson discloses “wherein the device is a cellular phone” as (see Abstract , a respective gateway device).

Claim Rejections - 35 USC § 103

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10. Claims 7 and 14 are rejected under 35 U.S.C.103(a) as being unpatentable over Anderson (patent Number: 6115819)(hereinafter Anderson) in view of Porter et al (Pub. No: US2003/0226029) (hereinafter Porter).

As per claim 7, **Anderson discloses** “The method of claim 1(see rejection above claim 1), **but fails expressly to disclose** "wherein the blocking function comprises changing the destination address of the data transferred to the working memory".

However, Porter discloses “ wherein the blocking function comprises changing the destination address of the data transferred to the working memory” as (page 5 , paragraph 0040, line 3-8, Memory controllers can also be used to change the address in which data is stored in memory. Unauthorized access to such configuration settings in memory controllers could result in the storage of data to un-secure portions of memory within memory).

Anderson and Porter are analogous arts because they are the same field of endeavor of system for protecting secure registers.

Therefore, It would have been obvious to one of the ordinary skill in the art at the time of the invention was made to modify the teaching of Anderson by including the changing address of the data while copying it from ROM to RAM that taught by Porter because it would provide a system for securely protecting security features within an information handling system would be useful in the inbuilt un trusted system(column 1, paragraph 0006, line 16-20).

As per claim 14, Anderson discloses “The device of claim 9” as (see rejection above claim 9), **but fails expressly to disclose** “wherein the blocking function of the monitoring unit comprises blocking write attempts by changing the destination address of the data transferred to the working memory”.

However, Porter discloses " wherein the blocking function of the monitoring unit comprises blocking write attempts by changing the destination address of the data transferred to the working memory" as (page 5 , paragraph 0040, line 3-8, Memory controllers can also be used to change the address in which data is stored in memory. Unauthorized access to such configuration settings in memory controllers could result in the storage of data to un-secure portions of memory within memory).

Anderson and Porter are analogous arts because they are the same field of endeavor of system for protecting secure registers or write protect working memory.

Therefore, It would have been obvious to one of the ordinary skill in the art at the time of the invention was made to modify the teaching of Anderson by including the changing address of the data while copying it from ROM to RAM that taught by Porter because it would provide a system for securely protecting security features within an information handling system would be useful in the inbuilt un trusted system(column 1, paragraph 0006, line 16-20).

11. Claim 17 is rejected under 35 U.S.C.103(a) as being unpatentable over Carey et al (patent Number: 4489380)(hereinafter Carey) in view of Anderson et al (Patent Number:6115819) (hereinafter Anderson).

As per claim 17, **Carey discloses** " a non-volatile memory comprising data including security data to be write-protected" as (column 2, line 11-13, The microprocessor generates signals to put the RAM into the write protect mode by setting a write protect flop); "a working memory" as (column 2, line 4-5, The RAM is operative on a read or write operation); **but fails to expressly discloses**, " a central processing unit configured to control copying of at least some data from the non-volatile memory to the working memory;and a device for blocking write attempts to security data transferred from the non-volatile memory to the working memory; and comprising a monitoring unit configured to : activate a blocking function for security data in the working memory , which activation is triggered by a copying of the security data being made from the non-volatile memory to the working memory; monitor all communication with the working memory; and block all write attempts to the copied security data stored in the working memory according to the blocking function , all performed independently of the central processing unit, such that the central processing unit cannot manipulate the security data".

However, Anderson discloses "a central processing unit configured to control copying of at least some data from the non-volatile memory to the working memory" as (column 6, line 15-19, exchanging data between various elements of the system) ; and "a device for blocking write attempts to security data transferred from the non-volatile memory to the working memory and comprising a monitoring unit configured to : activate a blocking function for

security data in the working memory , which activation is triggered by a copying of the security data being made from the non-volatile memory to the working memory" as (column 4, line 46-50, the Access monitor is being initiation at the time of copying data from ROM to Main RAM); " monitor all communication with the working memory" as (column 4, line 59-61, By monitoring the signals on the system bus the access monitor can determine the details of every data access that takes place) ; and " block all write attempts to the copied security data stored in the working memory according to the blocking function , all performed independently of the central processing unit, such that the central processing unit cannot manipulate the security data" as (column 6. line 46-48, The AM will allow or disallow the access to memory by controlling gate 44 to pass or not pass the read or write command, column 6, line 15-19,Restrictions on the exchange or transfer of data between various elements of the system is controlled by the Access monitor).

Carey and Porter are analogous arts because they are the same field of endeavor of system of generating an interrupt when a central processor unit attempts to write into a memory which is in a write protected mode.

Therefore, It would have been obvious to one of the ordinary skill in the art at the time of the invention was made to modify the teaching of Carey by including every access by the CPU to system memory is controlled by the Access monitor that taught by Anderson because it would provide a computer

hardware having inbuilt trusted functionality that would prevent to modify the data in the RAM in an untrusted computer(column 3, line 9-14).

12. Claim 23 is rejected under 35 U.S.C.103(a) as being unpatentable over Carey et al (patent Number: 4489380)(hereinafter Carey) in view of Anderson et al (Patent Number:6115819) (hereinafter Anderson) and further in view of Porter et al (Pub. No: US2003/0226029) (hereinafter Porter).

As per claim 23, **Carey in view of Anderson discloses** "The electronic data processing device of claim 17" as (see rejection above claim 17), **but fails to expressly disclose** " wherein the blocking function of the monitoring unit comprises blocking write attempts by changing the destination address of data transferred to the working memory"

However , **Porter discloses** " wherein the blocking function of the monitoring unit comprises blocking write attempts by changing the destination address of the data transferred to the working memory" as (page 5 , paragraph 0040, line 3-8, Memory controllers can also be used to change the address in which data is stored in memory. Unauthorized access to such configuration settings in memory controllers could result in the storage of data to un-secure portions of memory within memory).

Carey in view of Anderson and Porter are analogous arts because they are the same field of endeavor of system for protecting secure registers or write protected memory.

Therefore, It would have been obvious to one of the ordinary skill in the art at the time of the invention was made to modify the teaching of Carey in view of Anderson by including the Memory controllers that can change the address of data during storing into the RAM that taught by Porter because it would provide a system for securely protecting security features within an information handling system would be useful in the inbuilt un trusted system (column1, paragraph 0006, line 16-20).

Conclusion

13. The following prior art made of record and not relied upon is cited to establish the level of skill in the applicant's art and those arts considered reasonably pertinent to applicant's disclosure. See MPEP 707.05(c).

14. The following reference teaches execution of trial data.

US 4489380

US 6115819

US 2003/0226029

US 5825875

15. Any inquiry concerning this communication or earlier communication form the examiner should be directed to Abu Sholeman whose telephone number is (571)270-7314. the examiner can normally be reached on Monday to Friday 8:30 AM to 5.00PM.

If attempts to reach the above noted Examiner by telephone are un successful, the Examiner's supervisor, Thomas Pham, can be reached at the following telephone number (571)2272-3689.

The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from the either Private PAIR or public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pari-direct.uspto.gov. Should your have questions on access to the Private PAIR system, contact the Electronic Business Center(EBC) at 866-217-9197(toll-free).

October 15. 2008
/A.S./

Abu Sholeman
Examiner
Art Unit 4148

/THOMAS K PHAM/
Supervisory Patent Examiner, Art Unit 4148